FORM PTO-1390 (Modified) (REV 10-95) U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
197593US2PCT

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR
09/647547

INTERNATIONAL APPLICATION NO. **PCT/SE99/00516**	INTERNATIONAL FILING DATE **30 March 1999**	PRIORITY DATE CLAIMED **01 April 1998**

TITLE OF INVENTION
IMPROVEMENTS IN, OR RELATING TO, ELECTRONIC BADGES

APPLICANT(S) FOR DO/EO/US
Stefan GRINNEBY

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. □ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) at any time rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c) (2))
   a. □ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. □ is not required, as the application was filed in the United States Receiving Office (RO/US).
6. □ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ A copy of the International Search Report (PCT/ISA/210).
8. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3))
   a. □ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. □ have been transmitted by the International Bureau.
   c. □ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
9. □ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
10. □ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
11. ☒ A copy of the International Preliminary Examination Report (PCT/IPEA/409).
12. □ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 13 to 18 below concern document(s) or information included:

13. □ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
14. □ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
15. ☒ A **FIRST** preliminary amendment.
    A **SECOND** or **SUBSEQUENT** preliminary amendment.
16. □ A substitute specification.
17. □ A change of power of attorney and/or address letter.
18. □ Certificate of Mailing by Express Mail
19. ☒ Other items or information:

Request for Consideration of Documents Cited in International Search Report
Notice of Priority
PCT/IB/304
PCT/IB/308

U.S. APPLICATION NO. (IF KNOWN, SEE 37 CFR	INTERNATIONAL APPLICATION NO.	ATTORNEY'S DOCKET NUMBER
09/647547	PCT/SE99/00516	197593US2PCT

20. The following fees are submitted:.

				CALCULATIONS	PTO USE ONLY
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)) :					
□ Search Report has been prepared by the EPO or JPO			$860.00		
□ International preliminary examination fee paid to USPTO (37 CFR 1.482)			$690.00		
□ No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2))			$710.00		
☒ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2) paid to USPTO			$1000.00		
□ International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4)			$100.00		
ENTER APPROPRIATE BASIC FEE AMOUNT =				$1000.00	
Surcharge of **$130.00** for furnishing the oath or declaration later than □ 20 ☒ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).				$130.00	
CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	44 - 20 =	24	x $18.00	$432.00	
Independent claims	3 - 3 =	0	x $80.00		
Multiple Dependent Claims **(check if applicable).**			□	**$0.00**	
TOTAL OF ABOVE CALCULATIONS =				$1,562.00	
Reduction of 1/2 for filing by small entity, if applicable. Verified Small Entity Statement must also be filed (Note 37 CFR 1.9, 1.27, 1.28) **(check if applicable).**			□	**$0.00**	
SUBTOTAL =				$1,562.00	
Processing fee of **$130.00** for furnishing the English translation later than □ 20 □ 30 months from the earliest claimed priority date (37 CFR 1.492 (f)). +				**$0.00**	
TOTAL NATIONAL FEE =				$1,562.00	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31) **(check if applicable).**			□	**$0.00**	
TOTAL FEES ENCLOSED =				$1,562.00	
				Amount to be: refunded	$
				charged	$

☒ A check in the amount of $1,562.00 to cover the above fees is enclosed.

□ Please charge my Deposit Account No. in the amount of to cover the above fees. A duplicate copy of this sheet is enclosed.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. **15-0030** A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

22850

Surinder Sachar
Registration No. 34,423

Surinder Sachar
SIGNATURE

Marvin J. Spivak
NAME

24,913
REGISTRATION NUMBER

Oct 2 2000
DATE

197593US

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF: :

STEFAN GRINNEBY : ATTN: APPLICATION DIVISION

SERIAL NO: NEW U.S. PCT APPLICATION
(BASED ON PCT/SE99/00516):

FILED: HEREWITH :

FOR: IMPROVEMENTS IN, OR RELATING TO,
ELECTRONIC BADGES

PRELIMINARY AMENDMENT

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

Prior to a first examination on the merits, please amend the above-identified application as follows:

IN THE SPECIFICATION

Page 1, before line 1, insert

--TITLE OF THE INVENTION--;

between lines 1 and 2, insert

--BACKGROUND OF THE INVENTION

Field of the Invention--;

between lines 6 and 7, insert

--<u>Discussion of the Background</u>--;

between prenumbered lines 19 and 21, insert

--<u>SUMMARY OF THE INVENTION</u>--.

Page 7, between lines 22 and 23, insert

--<u>BRIEF DESCRIPTION OF THE DRAWINGS</u>--.

Page 8, between prenumbered lines 5 and 6, insert

--<u>DESCRIPTION OF THE PREFERRED EMBODIMENTS</u>--.

<u>IN THE CLAIMS</u>

Claim 4, line 1, change "any previous claim," to --claim 1,--.

Claim 5, line 1, change "any previous claim," to --claim 1,--.

Claim 7, line 1, change "either claim 5, or 6," to --claim 5,--.

Claim 8, line 1, change "any previous claim," to --claim 1,--.

Claim 12, line 1, change "any of claims 8 to 11," to --claim 8,--.

Claim 13, line 1, change "any of claims 8 to 12," to --claim 8,--.

Claim 14, line 1, change "any of claims 8 to 13," to --claim 8,--.

Claim 15, line 1, change "any of claims 8 to 14," to --claim 8,--.

Claim 19, line 1, change "any of claims 16 to 19," to --claim 16,--.

Claim 20, line 1, change "any of claims 16 to 19," to --claim 16,--.

Claim 22, line 1, change "either claim 20, or 21," to --claim 20,--.

Claim 23, line 1, change "any of claims 16 to 22," to --claim 16,--.

Claim 25, line 1, change "either claim 23, or 24," to --claim 23,--.

Claim 28, line 1, change "any of claims 24 to 27," to --claim 24,--.

Claim 29, line 1, change "any of claims 24 to 28," to --claim 24,--.

Claim 30, line 1, change "any of claims 24 to 29," to --claim 24,--.

Claim 31, line 1, change "any of claims 24 to 30," to --claim 24,--.

Claim 35, line 1, change "any of claims 32 to 34," to --claim 32,--.

Claim 36, line 1, change "any of claims 32 to 34," to --claim 32,--.

Claim 38, line 1, change "either claim 36, or 37," to --claim 36,--.

Claim 39, line 1, change "any of claims 32 to 38," to --claim 32,--.

Claim 43, line 1, change "any of claims 36 to 42," to --claim 36,--.

Claim 44, line 1, change "any of claims 36 to 42," to --claim 36,--.

REMARKS

Favorable consideration of this application, as presently amended, is respectfully requested.

The present preliminary amendment is submitted to place the above-identified application in more proper format under United States practice. By the present preliminary amendment the specification has been amended to include suggested headings. The claims have been amended to no longer recite any multiple dependencies.

The present application is believed to be in condition for a full and thorough examination on the merits. An early and favorable consideration of the present application is hereby respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Surinder Sachar

Gregory J. Maier
Attorney of Record
Registration No. 25,599
Surinder Sachar
Registration No. 34,423

22850

(703) 413-3000
Fax #: (703)413-2220
SNS/js

I:\atty\SNS\197593us-pr.wpd

3/PRTS

Improvements in, or Relating to, Electronic Badges

The present invention relates to a telecommunications system employing electronic security badges to provide temporary access to a computer system protected by firewalls, methods of providing temporary, controlled, access to a secure computer system, and an administration computer architecture for use with a telecommunications system employing electronic security badges.

With modem data communications technology, it is frequently desirable to give a site visitor access to a secure computer system over electronic transmission systems. For example, it may be desirable to hold a conference, or virtual meeting, in cyberspace, which is hosted on a secure computer, to which general public access is denied for security reasons. In such a meeting, it may be necessary for a visitor to run applications software on the host computer. However, the person hosting such a meeting may well wish to limit a visitor's access to a certain set of the applications available on the host computer. If access to the host computer is given to a visitor, this will, to some extent, compromise the security of the host computer, unless special steps are taken to protect the host computer.

Existing systems for providing access to computers protected by firewalls are either inflexible and difficult for a visitor to use, or ineffective in terms of preserving the security of the home computer.

The present invention makes an electronic visitor's badge available to a person visiting a host computer protected by firewalls, and solves the problem of providing flexible, user friendly, access without compromising security. The present invention permits persons located behind an address translating firewall, which only allows HTTP, to obtain controlled access to privileged data information without compromising data security. The badge establishes a reliable contact from which only trustworthy instructions will emanate, i.e. the instructions will only come from an approved and security cleared visitor.

Initial contact between a visitor and the host, i.e. an individual responsible for operation of the host computer, is established via a telephone conversation over the PSTN. Visitor and host agree on a password, or code word. The code is added, possibly in encrypted form, to the source code of an electronic badge. The electronic badge may be a Java applet which is compiled and placed on a webserver protected by the password. When this "applet" is run via port 80, i.e. the port used for communication through a firewall, the code in the control server is correlated to the code presented by the badge, in other words, it does not matter that the firewall between visitor and host has changed the IP address.

The present invention can be used in any situation where individuals wish to work on a common computer and it is not possible to exchange hardware, but the individuals are able to recognize each others voices. The invention facilitates secure control of access to a secure computer facility via exchange of identity badges over the Internet.

The present invention strengthens the link between three security elements:

- voice recognition;

- knowledge of a password; and

- possession of an electronic badge - i.e. an applet

and manages a translating/masking firewall, via port 80.

According to a first aspect of the present invention, there is provided a telecommunications system adapted to act as a platform for electronic meetings, comprises a visitor's computer, an administration computer, an application computer, a firewall protecting said application computer and a transmission path over the Internet, characterised in that communications between said visitor's computer and said application computer are mediated by an electronic badge generated by said administration computer and operating on said visitor's computer.

Said administration computer and application computer may be realised on a single data processing machine.

Alternatively, said administration computer and application computer may be distinct data processing machines, and communications between said visitor's computer and said application computer may be controlled by a firewall located in said administration computer.

Said administration computer may be protected by a firewall.

Said electronic badge may be an applet containing data identifying a visitor, a password, and a list of access rights relating to software applications running on said application computer.

Said list of access rights may permit access to one, or more, software applications.

Said applet may be adapted to run on said visitor's computer and cause one, or more, icons to be displayed on a VDU associated with said visitor's computer.

Said administration computer may include a control panel linked to a web server adapted to issue electronic badges.

Said administration computer may include a control server linked to said control panel and said web server, and a database of access rules linked to said control server.

Said control server may be linked to a firewall protecting said application computer, and said database of access rules may be linked to said firewall protecting said application computer.

Access to said webserver may be controlled by a password protection means.

An electronic visitor's badge may be created from said control panel and deposited for collection on said webserver.

Said visitor's computer may download said electronic visitor's badge by accessing said web server and giving a password and visitor identification.

Access rights associated with said visitor's badge may be altered while said visitor computer is connected to said application computer.

Said visitor's badge may be adapted to self destruct on receipt of a signal from said control server.

According to a second aspect to the present invention, there is provided a method of establishing access for a visitor's computer to an application computer protected by a firewall generated by an administration computer, over the Internet, characterised by mediating communications between said visitor's computer and said application computer with an electronic badge generated on said administration computer and operating on said visitor's computer.

Said administration computer and said application computer may be realised on a single data processing machine.

Said administration computer and application computer may be realised as distinct data processing machines, and communications between said visitor's computer and said application computer may be controlled through a firewall located in said administration computer.

Said administration computer may be protected with a firewall.

Said electronic badge may be an applet containing data identifying a visitor, a password, and a list of access rights relating to software applications running on said application computer.

Said list of access rights may permit access to one, or more, software applications.

Said applet may run on said visitor's computer and cause one, or more, icons to be displayed on a VDU associated with said visitor's computer.

Said administration computer may include a control panel linked to a web server adapted to issue electronic badges.

The method may include the steps of:

- establishing a voice link over the PSTN between a person operating said visitor's computer, herein referred to as a visitor, and a person operating said administration computer, herein referred to as a host;

- said host establishing that said visitor has clearance to access said application computer, and

- assigning and communicating a password to said visitor over said voice link.

Said administration computer may include a control server linked to said control panel and said web server, and a database of access rules linked to said control server.

Said control server may be linked to a firewall protecting said application computer, and said database of access rules may be linked to said firewall protecting said application computer.

Access to said webserver may be controlled by a password protection means.

Said host may create an electronic visitor's badge by actuation of said control panel and depositing said electronic visitor's badge, for collection by said visitor, on said webserver.

Said visitor may access said webserver over the Internet, giving said password, and downloading said electronic visitor's badge.

Said method may include the steps of:

- said visitor requesting access, while connected to said application computer, to a first software application, not pre-authorised on said electronic visitor's badge;

- said control panel giving an alarm condition;

- said host confirming over said voice link that said visitor has requested access to said first software application; and

- modifying the access rights associated with said electronic visitor's badge via said control panel.

Said visitor's badge may self destruct on receipt of a signal from said control server.

According to a third aspect of the present invention, there is provided an administration computer, for use with a telecommunications system adapted to act as a platform for electronic meetings, said administration computer having a firewall protecting an application computer, characterised in that said administration computer is adapted to create an electronic badge to mediate communications between a visitor's computer and said application computer.

Said administration computer and application computer may be realised on a single data processing machine.

Said administration computer and application computer may be distinct data processing machines.

Said administration computer may be protected by a firewall.

Said electronic badge may be an applet containing data identifying a visitor, a password, and a list of access rights relating to software applications running on said application computer.

Said list of access rights may permit access to one, or more, software applications.

Said applet may be adapted to run on said visitor's computer and cause one, or more, icons to be displayed on a VDU associated with said visitor's computer.

Said administration computer may include a control panel linked to a web server adapted to issue electronic badges.

Said administration computer may include a control server linked to said control panel and said web server, and a database of access rules linked to said control server.

Said control server may be linked to a firewall protecting said application computer, and said database of access rules may be linked to said firewall protecting said application computer.

Access to said webserver may be controlled by a password protection means.

An electronic visitor's badge may be created from said control panel and deposited for collection on said webserver.

Access rights associated with said visitor's badge may be altered while a visitor computer is connected to said application computer.

Embodiments of the invention will now be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 illustrates, in schematic form, an overview of a telecommunications system, according to the present invention.

Figure 2 illustrates, in greater detail, the administration computer and application computer of Figure 1.

Figure 3 illustrates, in greater detail, the participator computer of Figure 1.

The system of the present invention may include seven main components, namely:

- a control server, 6, see the accompanying drawings;
- a control panel, 4;
- a visitor's badge, in the form of an applet, 9;
- firewalls, 17, 24 and 7;
- a webserver, 5;
- a PSTN telephone link, 1,2 and 3; and
- applications software, 13, 14 and 15.

As illustrated in the accompanying drawings, a telecommunications system which supports secure communication between a visitor's, or participator's, computer, 8, and application, or host computer, 24, has an administration computer 19. The participator computer, 8, is linked via a firewall, 17, to the Internet 18, and thence through firewall, 24, to the administration computer 19. The administration computer, 19, includes a webserver, 5, for issuing visitor's badges in the form of Java applets, and is protected by a password recognition unit, 20. The administration computer includes a control panel, 4, which may take the form of a visual screen based interface, allowing an operator to control the administration computer and the issue of electronic badges. Each badge is in the form of an applet which, when run on a visitor's computer, such as 8, includes a series of icons for a range of applications on the application computer, to which the visitor is given access rights by the electronic badge. In the case of the embodiment illustrated in the drawings, these applications include applications 13, 14, and 15 which might be MS-Netmeeting, Word 6, and Coral Draw 6.

The administration computer also includes a control server, 6, which controls a server, 16, carrying the access rules for the application computer, 34, and the firewall, 7, which protects the application computer. Access to the individual applications packages 13, 14, and 15, is controlled individually via the firewall, so that access may be granted to one, two, or all of applications 13 to 15, depending on the access rights granted to a given electronic visitor's badge. Access rights associated with an electronic badge may be altered during the course of a meeting, or conference, via the control panel and control server, giving true dynamic control.

In operation, a visitor and host speak to each other over the telephone link 1, 3, 2. They agree a password and the access rights the visitor will have. The host may identify the visitor by his/her voice, or by exchange of personal information, a PIN number, or the like. Once identification has been established to the satisfaction of the host, a password is issued orally to the visitor. The host then set ups an electronic visitor's badge for the host on the webserver 5, including the agreed password and the agreed access rights for the visitor. The electronic visitor's badge now resides on webserver 5 and awaits collection by the visitor.

The visitor can now set up a data link over the Internet to control server, 6 on a channel 24. It should be noted that the different communications channels 24, 35, 27,26 and 25 are labelled for easy identification in the drawings and may, in fact, represent à single communications link. The visitor is then requested to give her/his password, which is authenticated by the password protection unit 20, which, in turn, permits the electronic badge to be transmitted to the visitor's computer. On receipt by the visitor's computer, the electronic password, which as previously stated is a Java applet, runs on the visitor's computer. The electronic badge causes a number of icons to be displayed on the visitor's computer, 10, 11, and 12. By actuating the icons, the visitor obtains access via firewall 7, to the applications 13, 14 and 15 running on the application computer 34. The firewall operates to control the applications and data files to which the visitor can obtain access in accordance with the password instructions encoded in the electronic visitor's badge and the access rules held on server 16, all of which can be controlled via the control server 6, and control panel 4.

Although, as illustrated in the drawings, the administration computer, 19, and the application computer, 34, may be distinct data processing machines, it is also possible to realise both computers on a single data processing machine.

Consider the following scenario.

Two persons, a visitor and host, agree to hold a meeting over Internet. The host has, at his disposal, a computer system called the Control Lab Room System, and is prepared to host the meeting on this computer. On the telephone, the host and the visitor agree on the name and password for a visitor's badge which will then be created. The host sits by the control panel of the Control Lab Room System and creates this visitor's badge, and at this stage connects certain privileges to the badge. For example, the visitor will be allowed, on showing his/her badge, the right to use the MS-Netmeeting software available on the application computer. The visitor's badge is lodged on the webserver which belongs to the system. The visitor then draws and activates the badge via a special website, the reception. The name and password to get access to the badge are those which the host and the visitor have agreed on the telephone. The host will see when the badge has been activated, via the control panel and, if the host gives a receipt for the activation, the conference will commence. The visitor's badge has control codes which enable the visitor to request access to a range of functions available on the application computer, e.g. video, or a protected webserver. The host and the visitor start by using MS_Netmeeting. Since the host created the visitor's badge with rights for this equipment, it will start without any fresh intervention via the control panel.

After a while, however, the visitor wants to establish a connection with a video camera which shows the host's conference room. Before he/she has requested permission to do this, he/she starts his/her video client. When this happens, the control panel displays an alarm message, which shows that a visitor is trying to use a function for which the visitor has not been granted access rights. The host now asks the visitor, via the telephone link, if the attempt emanated from the visitor and, on receipt of a positive response, allocates, via a simple button press, the visitor with the right to establish the connection.

Now, suppose a hacker, called Charlie, tries to get access to the same video channel. Earlier in the week Charlie had intercepted IP-traffic which contained a visitor's badge. However, when he tried to use the badge, the host immediately identified the badge as time expired, and immediately excluded him from the conference. This time Charlie tries to steal the visitor's video flow. He is stopped once again, this time because the control server of the Control Lab Room System does not succeed in communicating with the visitor's badge which all authorized visitors must have. This causes a new alarm to be given. If the visitor, via the telephone, does not affirm that he has just opened a new client session, and the host is not satisfied that this second session also belongs to the visitor, the host refuses connection. Furthermore, the host will ignore all inquiries from that source for the remainder of the conference. The rest of the conference turns out well and, at the end of the conference, the host withdraws the visitor's badge by means of the control server, via its channel to the badge, issuing an instruction to the badge to self destruct.

In slightly more technical detail the course of events can be explained as follows.

The firewall informs the control server of an attempt to establish a connection which, based on pre-existing rules, the status of the visitor's badge and user control from the control panel, accepts, or denies, the connection, by creating a rule for the firewall to follow for this and similar connection attempts.

The visitor's badge is the critical point. Because it is an applet, it must be shown in a webreader on the visitor's screen in order to execute. If it is clicked away, it stops executing, and with that ceases to be valid. The source code of the visitor's badge includes the visitor's identity, together with the time period(s) for which it is valid. It must show this information to make the control server accept a connection from it and, implicitly, from the location from which a person attempts to access the application computer.

The control server is the hub of the system. The control server creates the visitor's badge in accordance with instructions received from the control panel and places the visitor's badge on the webserver as described above. When the badge has been drawn from the webserver, it establishes contact with the control server. If the badge is still active, all manipulations the host performs with the badge on the control panel are reflected on the badge at the visitor's computer, and vice verse. The control server also controls the firewall, which provides the security for the conference.

The firewall has a number of rules to follow, like all firewalls. The difference here is that the host can dynamically change these rules, based on:

- judgment of the telephone part of the conference; and
- the guarantee the visitor's badge gives about the identity of the person operating the computer connected through, or seeking connection through, the firewall.

The control panel gives the host a view of the whole system. All badges which have been distributed can be seen here, together with the functions that are active. All events which the host can influence in the system are shown on the control panel via the same interface as the visitor has, i.e. the badge.

CLAIMS

1. A telecommunications system adapted to act as a platform for electronic meetings, comprising a visitor's computer, an administration computer, an application computer, a firewall protecting said application computer and a transmission path over the Internet, characterised in that communications between said visitor's computer and said application computer are mediated by an electronic badge generated by said administration computer and operating on said visitor's computer.

2. A telecommunications system, as claimed in claim 1, characterised in that said administration computer and application computer are realised on a single data processing machine.

3. A telecommunications system, as claimed in claim 1, characterised in that said administration computer and application computer are distinct data processing machines, and in that communications between said visitor's computer and said application computer are controlled by a firewall located in said administration computer.

4. A telecommunications system, as claimed in any previous claim, characterised in that said administration computer is protected by a firewall.

5. A telecommunications system, as claimed in any previous claim, characterised in that said electronic badge is an applet containing data identifying a visitor, a password, and a list of access rights relating to software applications running on said application computer.

6. A telecommunications system as claimed in claim 5, characterised in that said list of access rights may permit access to one, or more, software applications.

7. A telecommunications system, as claimed in either claim 5, or 6, characterised in that said applet is adapted to run on said visitor's computer and

cause one, or more, icons to be displayed on a VDU associated with said visitor's computer.

8. A telecommunications system, as claimed in any previous claim, characterised in that said administration computer includes a control panel linked to a web server adapted to issue electronic badges.

9. A telecommunications system, as claimed in claim 8, characterised in that said administration computer includes a control server linked to said control panel and said web server, and a database of access rules linked to said control server.

10. A telecommunications system, as claimed in claim 9, characterised in that said control server is linked to a firewall protecting said application computer, and in that said database of access rules is linked to said firewall protecting said application computer.

11. A telecommunications system, as claimed in claim 10, characterised in that access to said webserver is controlled by a password protection means.

12. A telecommunications system, as claimed in any of claims 8 to 11, characterised in that an electronic visitor's badge can be created from said control panel and deposited for collection on said webserver.

13. A telecommunications system, as claimed in any of claims 8 to 12, characterised in that said visitor's computer can download said electronic visitor's badge by accessing said web server and giving a password and visitor identification.

14. A telecommunications system, as claimed in any of claims 8 to 13, characterised in that access rights associated with said visitor's badge can be altered while said visitor computer is connected to said application computer.

15. A telecommunications system, as claimed in any of claims 8 to 14, characterised in that said visitor's badge is adapted to self destruct on receipt of a

signal from said control server.

16. A method of establishing access for a visitor's computer to an application computer protected by a firewall generated by an administration computer, over the Internet, characterised by mediating communications between said visitor's computer and said application computer with an electronic badge generated on said administration computer and operating on said visitor's computer.

17. A method, as claimed in claim 16, characterised by realising said administration computer and said application computer on a single data processing machine.

18. A method, as claimed in claim 16, characterised by realising said administration computer and application computer as distinct data processing machines, and by controlling communications between said visitor's computer and said application computer through a firewall located in said administration computer.

19. A method, as claimed in any of claims 16 to 19, characterised by protecting said administration computer with a firewall.

20. A method, as claimed in any of claims 16 to 19, characterised by said electronic badge being an applet containing data identifying a visitor, a password, and a list of access rights relating to software applications running on said application computer.

21. A method, as claimed in claim 20, characterised by said list of access rights permitting access to one, or more, software applications.

22. A method, as claimed in either claim 20, or 21, characterised by said applet running on said visitor's computer and causing one, or more, icons to be displayed on a VDU associated with said visitor's computer.

23. A method, as claimed in any of claims 16 to 22, characterised by said administration computer including a control panel linked to a web server adapted

to issue electronic badges.

24. A method, as claimed in claim 23, characterised by the steps of:

- establishing a voice link over the PSTN between a person operating said visitor's computer, herein referred to as a visitor, and a person operating said administration computer, herein referred to as a host;

- said host establishing that said visitor has clearance to access said application computer, and

- assigning and communicating a password to said visitor over said voice link.

25. A method, as claimed in either claim 23, or 24, characterised by said administration computer including a control server linked to said control panel and said web server, and a database of access rules linked to said control server.

26. A method, as claimed in claim 25, characterised by said control server being linked to a firewall protecting said application computer, and by said database of access rules being linked to said firewall protecting said application computer.

27. A method, as claimed in claim 26, characterised by controlling access to said webserver with a password protection means.

28. A method, as claimed in any of claims 24 to 27, characterised by said host creating an electronic visitor's badge by actuation of said control panel and depositing said electronic visitor's badge, for collection by said visitor, on said webserver.

29. A method, as claimed in any of claims 24 to 28, characterised by said visitor accessing said webserver over the Internet, giving said password, and downloading said electronic visitor's badge.

30. A method, as claimed in any of claims 24 to 29, characterised by the steps of:

- said visitor requesting access, while connected to said application computer, to a first software application, not pre-authorised on said electronic visitor's badge;

- said control panel giving an alarm condition;

- said host confirming over said voice link that said visitor has requested access to said first software application; and

- modifying the access rights associated with said electronic visitor's badge via said control panel.

31. A method, as claimed in any of claims 24 to 30, characterised by said visitor's badge self destructing on receipt of a signal from said control server.

32. An administration computer, for use with a telecommunications system adapted to act as a platform for electronic meetings, said administration computer having a firewall protecting an application computer, characterised in that said administration computer is adapted to create an electronic badge to mediate communications between a visitor's computer and said application computer.

33. An administration computer, as claimed in claim 32, characterised in that said administration computer and application computer are realised on a single data processing machine.

34. An administration computer, as claimed in claim 32, characterised in that said administration computer and application computer are distinct data processing machines.

35. An administration computer, as claimed in any of claims 32 to 34, characterised in that said administration computer is protected by a firewall.

36. An administration computer, as claimed in any of claims 32 to 34, characterised in that said electronic badge is an applet containing data identifying a visitor, a password, and a list of access rights relating to software applications running on said application computer.

37. An administration computer as claimed in claim 36, characterised in that said list of access rights may permit access to one, or more, software applications.

38. An administration computer, as claimed in either claim 36, or 37, characterised in that said applet is adapted to run on said visitor's computer and cause one, or more, icons to be displayed on a VDU associated with said visitor's computer.

39. An administration computer, as claimed in any of claims 32 to 38, characterised in that said administration computer includes a control panel linked to a web server adapted to issue electronic badges.

40. An administration computer, as claimed in claim 39, characterised in that said administration computer includes a control server linked to said control panel and said web server, and a database of access rules linked to said control server.

41. An administration computer, as claimed in claim 40, characterised in that said control server is linked to a firewall protecting said application computer, and in that said database of access rules is linked to said firewall protecting said application computer.

42. An administration computer, as claimed in claim 41, characterised in that access to said webserver is controlled by a password protection means.

43. An administration computer, as claimed in any of claims 36 to 42, characterised in that an electronic visitor's badge can be created from said control panel and deposited for collection on said webserver.

44. An administration computer, as claimed in any of claims 36 to 42, characterised in that access rights associated with said visitor's badge can be altered while a visitor computer is connected to said application computer.

ABSTRACT

Improvements In, or Relating to, Electronic Badges

The present invention makes an electronic visitor's badge available to a person visiting a host computer protected by firewalls, and solves the problem of providing flexible, user friendly, access without compromising security. The present invention permits persons located behind an address translating firewall, which only allows HTTP, to obtain controlled access to privileged data information without compromising data security. The badge establishes a reliable contact from which only trustworthy instructions will emanate, i.e. the instructions will only come from an approved and security cleared visitor. Initial contact between a visitor and the host, i.e. an individual responsible for operation of the host computer, is established via a telephone conversation over the PSTN. Visitor and host agree on a password, or code word. The code is added, possibly in encrypted form, to the source code of an electronic badge. The electronic badge may be a Java applet which is compiled and placed on a webserver protected by the password. When downloaded onto a visitor's computer, the electronic badge mediates communication between the visitor's computer and a protected host computer. The present invention can be used in any situation where individuals wish to work on a common computer and it is not possible to exchange hardware, but the individuals are able to recognize each others voices. The invention facilitates secure control of access to a secure computer facility via exchange of identity badges over the Internet.

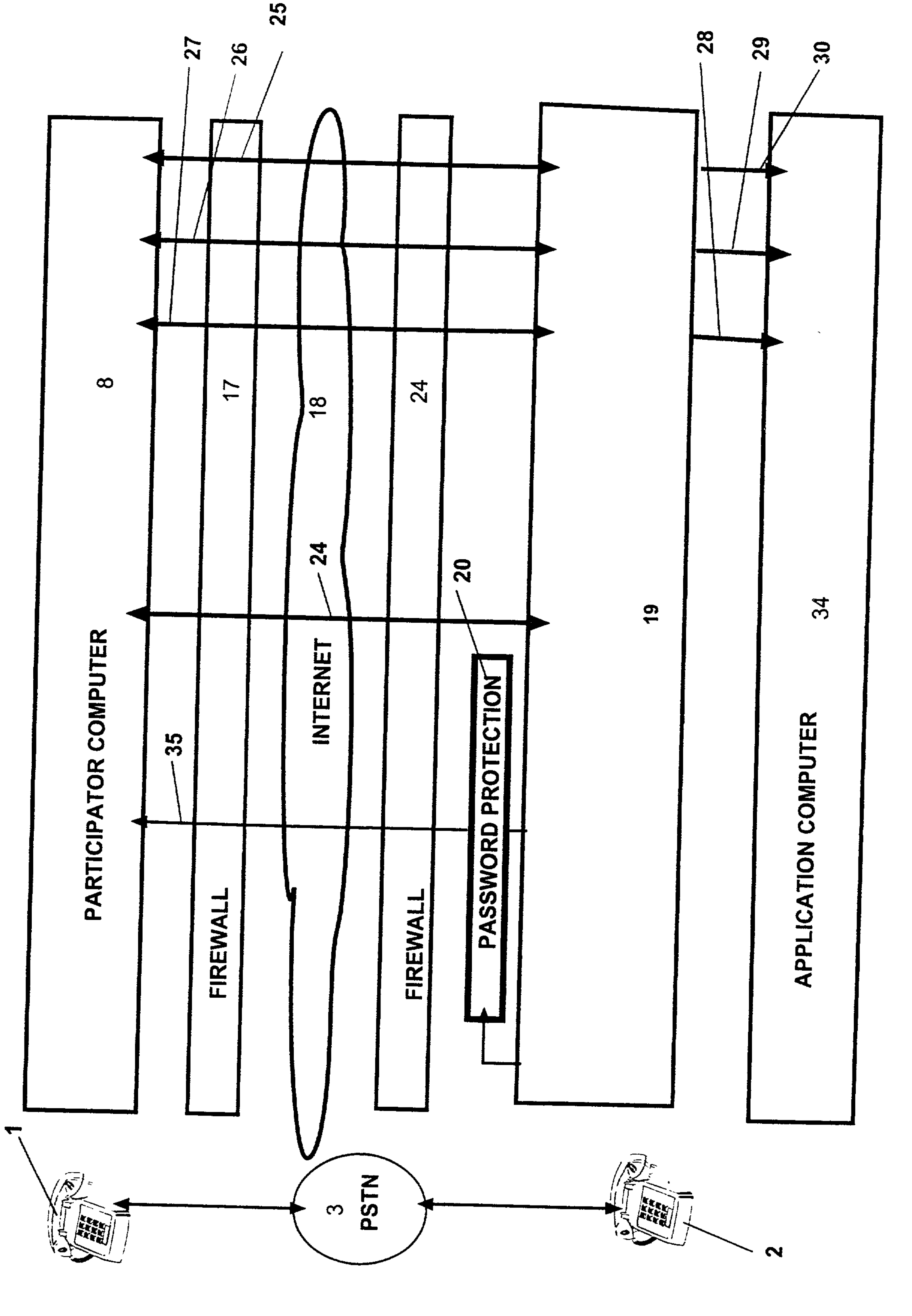
PARTICIPATOR COMPUTER
8
FIREWALL
17
INTERNET
18
24
FIREWALL
24
PASSWORD PROTECTION
20
19
APPLICATION COMPUTER
34
25
26
27
28
29
30
35
1
3
PSTN
2

FIGURE 1

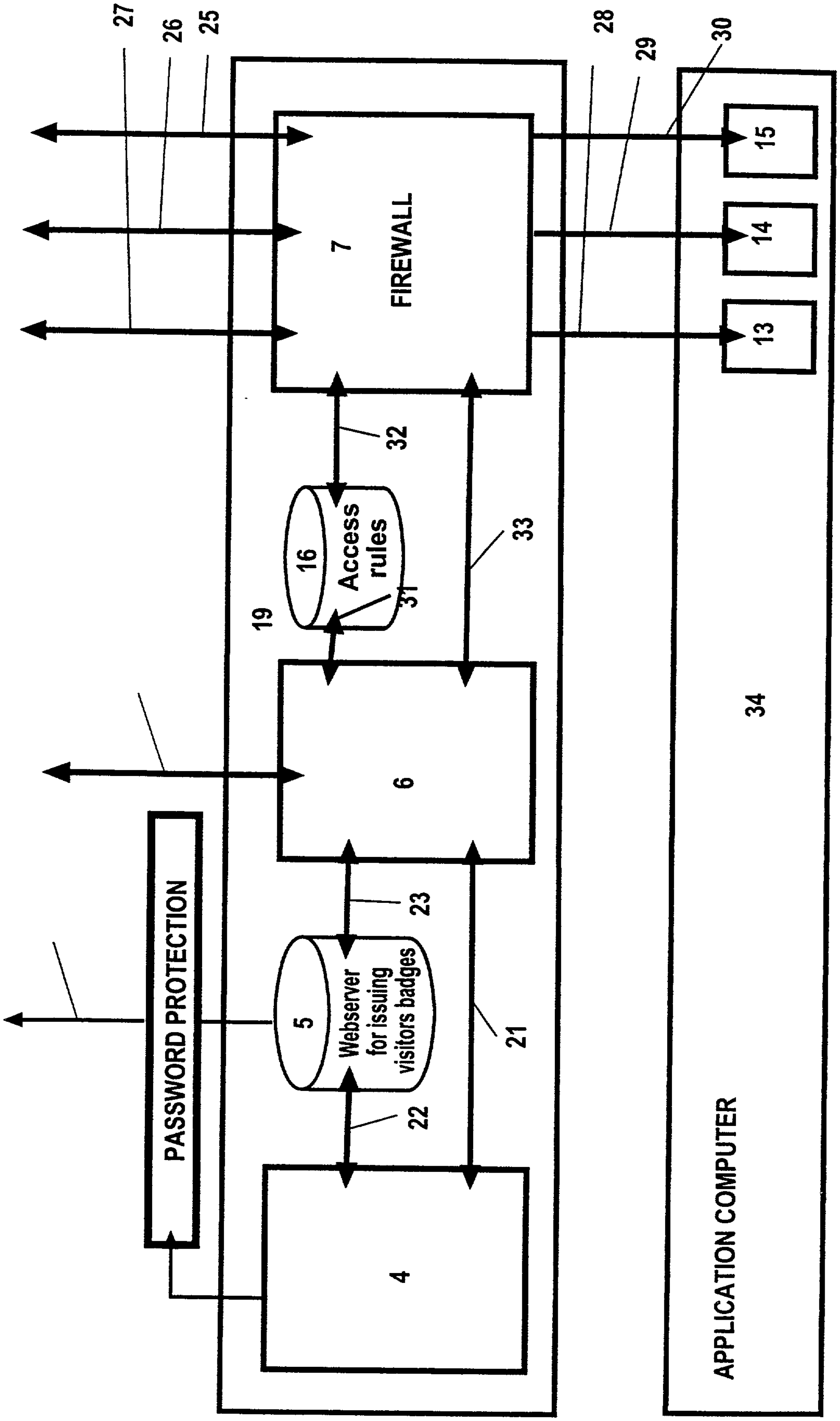
27
26
25
28
29
30
7
FIREWALL
15
14
13
32
16
Access rules
31
33
19
6
34
23
PASSWORD PROTECTION
5
Webserver for issuing visitors badges
21
22
4
APPLICATION COMPUTER

FIGURE 2

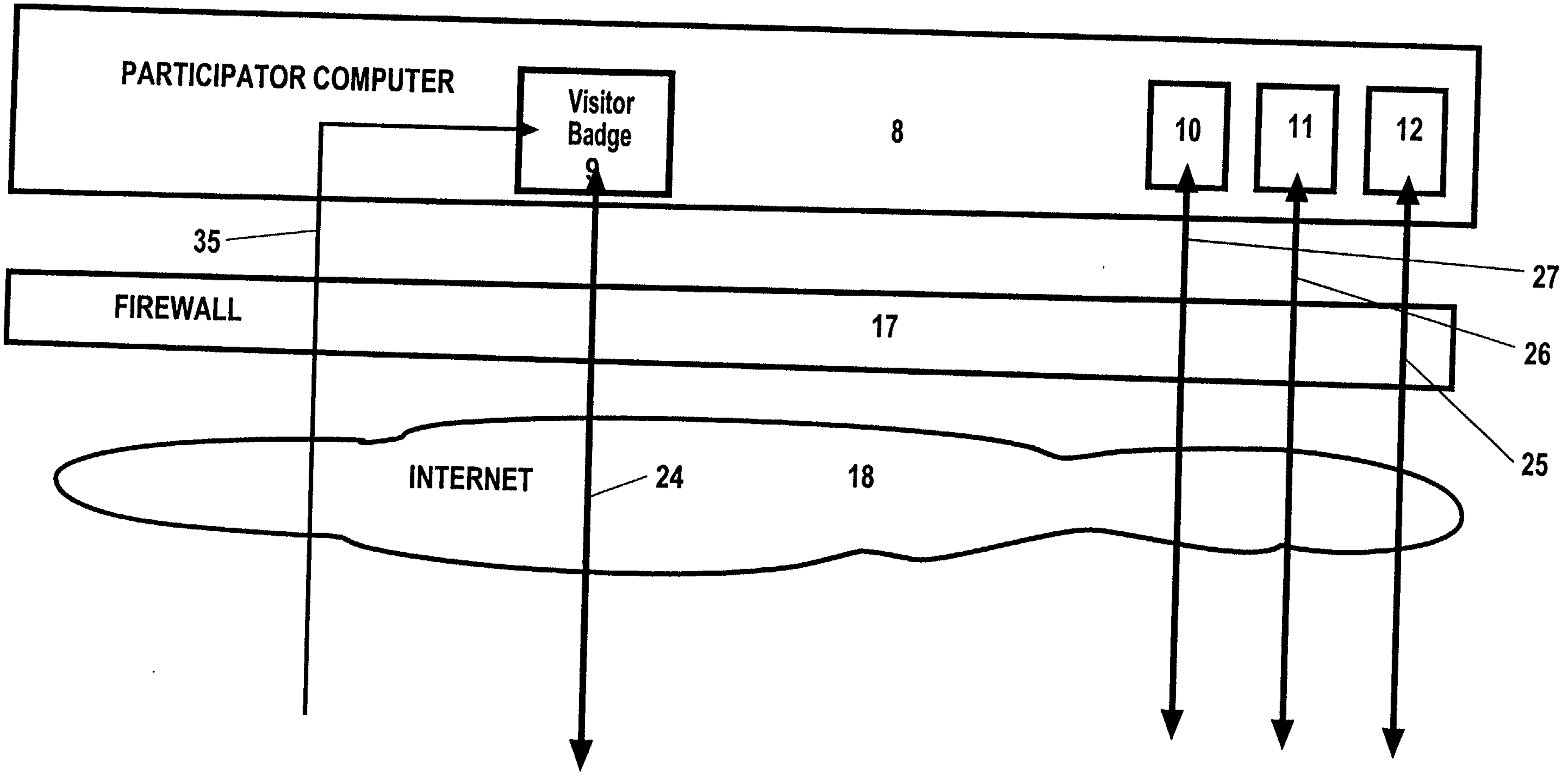
PARTICIPATOR COMPUTER
Visitor Badge
9
8
10
11
12
35
27
26
25
FIREWALL
17
INTERNET
24
18

FIGURE 3

Declaration, Power Of Attorney and Petition

WE (I) the undersigned inventor(s), hereby declare(s) that:

My residence, post office address and citizenship are as stated below next to my name,

We (I) believe that we are (I am) the original, first, and joint (sole) inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention entitled

IMPROVEMENTS IN, OR RELATING TO, ELECTRONIC BADGES

the specification of which

□ is attached hereto.

☒ was filed on 02 October 2000 as

Application Serial No. ______

and amended on ______.

□ was filed as PCT international application

Number PCT/SE99/00516

on March 30, 1999,

and was amended under PCT Article 19

on ______ (if applicable).

We (I) hereby state that we (I) have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

We (I) acknowledge the duty to disclose information known to be material to the patentability of this application as defined in Section 1.56 of Title 37 Code of Federal Regulations.

We (I) hereby claim foreign priority benefits under 35 U.S.C. § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate, or § 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate, or PCT International application having a filing date before that of the application on which priority is claimed. Prior Foreign Application(s)

Application No.	Country	Day/Month/Year	Priority Claimed
9801151-3	SWEDEN	01 April 1998	☒ Yes □ No
			□ Yes □ No
			□ Yes □ No
			□ Yes □ No

We (I) hereby claim the benefit under Title 35, United States Code, § 119(e) of any United States provisional application(s) listed below.

(Application Number)	(Filing Date)
(Application Number)	(Filing Date)

We (I) hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s), or § 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application.

Application Serial No.	Filing Date	Status (pending, patented, abandoned)
PCT/SE99/00516	30 March 1999	

And we (I) hereby appoint: Norman F. Oblon, Reg. No. 24,618; Marvin J. Spivak, Reg. No. 24,913; C. Irvin McClelland, Reg. No. 21,124; Gregory J. Maier, Reg. No. 25,599; Arthur I. Neustadt, Reg. No. 24,854; Richard D. Kelly, Reg. No. 27,757; James D. Hamilton, Reg. No. 28,421; Eckhard H. Kuesters, Reg. No. 28,870; Robert T. Pous, Reg. No. 29,099; Charles L. Gholz, Reg. No. 26,395; William E. Beaumont, Reg. No. 30,996; Jean-Paul Lavalleye, Reg. No. 31,451; Stephen G. Baxter, Reg. No. 32,884; Richard L. Treanor, Reg. No. 36,379; Steven P. Weihrouch, Reg. No. 32,829; John T. Goolkasian, Reg. No. 26,142; Richard L. Chinn, Reg. No. 34,305; Steven E. Lipman, Reg. No. 30,011; Carl E. Schlier, Reg. No. 34,426; James J. Kulbaski, Reg. No. 34,648; Richard A. Neifeld, Reg. No. 35,299; J. Derek Mason, Reg. No. 35,270; Surinder Sachar, Reg. No. 34,423; Christina M. Gadiano, Reg. No. 37,628; Jeffrey B. McIntyre, Reg. No. 36,867; William T. Enos, Reg. No. 33,128; Michael E. McCabe, Jr., Reg. No. 37,182; Bradley D. Lytle, Reg. No. 40,073; and Michael R. Casey, Reg. No. 40,294; our (my) attorneys, with full powers of substitution and revocation, to prosecute this application and to transact all business in the Patent Office connected therewith; and we (I) hereby request that all correspondence regarding this application be sent to the firm of OBLON, SPIVAK, McCLELLAND, MAIER & NEUSTADT, P.C., whose Post Office Address is: Fourth Floor, 1755 Jefferson Davis Highway, Arlington, Virginia 22202.

29

We (I) declare that all statements made herein of our (my) own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

1-00

Stefan GRINNEBY
NAME OF FIRST SOLE INVENTOR

Signature of Inventor

2000-12-27
Date

Residence: Rindögatan 15.6
S-115 36 Stockholm, Sweden
SEX

Citizen of: Sweden

Post Office Address: Same as above